Adam J. Zapala (SBN 245748)
Reid Gaa (SBN 330141)
COTCHETT, PITRE & McCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577
azapala@cpmlegal.com;
rgaa@cpmlegal.com

Scott C. Nehrbass *(pro hac vice)*
Daniel J. Buller *(pro hac vice)*
FOULSTON SIEFKIN LLP
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway
Overland Park, KS 66210-2000
Tel: (913) 253-2144
Fax: (866) 347-1472
snehrbass@foulston.com; dbuller@foulston.com

E. Powell Miller *(pro hac vice)*
Sharon S. Almonrode *(pro hac vice)*
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com; ssa@millerlawpc.com

[Additional counsel listed on signature page]
Attorneys for Plaintiffs and the Putative Class

Hassan A. Zavareei (SBN 181547)
Mark Clifford *(pro hac vice)*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, DC 20036
Tel: (202) 973-0900
Fax: (202) 973-0950
hzavareei@tzlegal.com;
mclifford@tzlegal.com

Jennie Lee Anderson (SBN 203586)
ANDRUS ANDERSON LLP
155 Montgomery Street, Suite 900
San Francisco, CA 94104
Tel: (415) 986-1400
Fax: (415) 986-1474
jennie@andrusanderson.com

Elizabeth A. Fegan *(pro hac vice)*
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Tel: (312) 741-1019
Fax: (312) 264-0100
beth@feganscott.com

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

I.C., a minor, by and through his natural parent, NASIM CHAUDHRI, AMY GITRE, CAROL JOHNSON, LISA THOMAS, JOSEPH MARTINEZ IV, DANIEL PETRO, and CHRISTOPHER ROSIAK, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ZYNGA, INC.,

Defendant.

Case No. 4:20-cv-01539-YGR

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiffs I.C., a minor, by and through his natural parent, Nasim Chaudhri, Amy Gitre, Carol Johnson, Lisa Thomas, Joseph Martinez IV, Daniel Petro, and Christopher Rosiak (collectively, "Plaintiffs"), individually and on behalf of all other persons similarly situated, by and through their undersigned counsel, for their Complaint against Defendant Zynga, Inc., allege as follows, based upon personal knowledge and on information and belief derived from, among other things, Zynga's September 12, 2019 "Player Security Announcement," investigation of counsel, media reports, and review of public documents:

I. INTRODUCTION

1. Defendant Zynga, Inc. ("Zynga" or "Defendant") proclaims itself "a leading developer of the world's most popular social games that are played by millions of people around the world each day." Zynga promises that it has in place "reasonable and appropriate security measures to help protect the security of your information both online and offline and to ensure that your data is treated securely…."

2. In fact, hundreds of millions of people, including Plaintiffs, trusted and believed Zynga's promise to protect their personally identifying information, including name, email address, Zynga ID and password, Facebook ID and password and, in some instances, financial information given to Zynga for purchases for games and other in-game items (collectively, "PII").[1]

3. Yet despite its promise, Zynga failed to protect its customers' PII by, among other things, using outdated password encryption methods that were banned for use by federal governmental agencies as early as 2010.

4. In September of 2019, Zynga's customer data base was breached by a serial hacker who had previously stolen and sold PII on the dark web. By current estimates, the PII of over 170 million Zynga account holders was accessed (the "Zynga Data Breach" or "Data Breach"). Although Zynga had notice of the breach and identified which of its customer accounts were accessed, Zynga never directly notified those customers.

[1] As used throughout this Complaint, "PII" is defined as all information exposed by the Zynga Data Breach that occurred on or around September 2019, including but not limited to all or any part or combination of name, address, telephone number, email address, gender, Zynga login and password, Facebook login and password, credit card information, and other personally identifying information.

5. Since the Zynga Data Breach, Zynga's customers have been exposed to credit and identity theft, "credit stuffing," phishing scams, and other illegal and fraudulent conduct perpetrated by the criminal actors who have come into possession of the stolen PII, either through purchase of the same on the Dark Web or through the theft of the PII during the Data Breach itself. Plaintiffs have and will incur costs to mitigate the risk for the Data Breach, such as paying for credit monitoring services, and will have to spend countless hours monitoring their credit reports and credit card statements. Regardless of whether they have yet to incur out-of-pocket losses, Plaintiffs and all Zynga customers whose PII was stolen remain subject to a pervasive, substantial, and imminent risk of identity theft and fraud now and for years to come.

6. This class action is brought on behalf of all persons residing in the United States whose PII was compromised in the Zynga Data Breach to redress the damages they have suffered and to obtain appropriate equitable relief to mitigate the risk that Zynga will be breached in the future.

II. PARTIES

7. Plaintiff I.C., a minor, by and through his natural parent, Nasim Chaudhri, is a resident and citizen of Kansas. Plaintiff provided his PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

8. Plaintiff I.C., a minor, by and through his natural parent, Nasim Chaudhri, played Zynga games from approximately mid-2018 until learning of the Data Breach, and the games included *Words With Friends*. I.C.'s PII was stolen in the Zynga Data Breach as confirmed through the website haveibeenpwned.com. I.C. did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. I.C. has not played *Words With Friends* or any other Zynga game since learning of the Data Breach, has no intention of logging in to or accessing any Zynga game in the future, and has not retained any benefits from any agreement that Zynga may claim exists, nor does he intend to do so in the future. I.C. no longer accesses *Words With Friends* or any other Zynga product to his knowledge.

9. Plaintiff I.C., a minor, by and through his natural parent, Nasim Chaudhri, disaffirms, repudiates, nullifies, and wishes not to be bound by any and all contracts claimed by Zynga, including the arbitration agreement, terms of service, delegation clause, and all other agreements claimed by Zynga.

10. Plaintiff Amy Gitre is a resident and citizen of Michigan. Plaintiff provided her PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

11. Plaintiff Amy Gitre's PII was stolen in the Zynga Data Breach. Plaintiff did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. Plaintiff Gitre played both *Words With Friends* and *Wizard of Oz Slots*.

12. Plaintiff Carol Johnson is a resident and citizen of Missouri and at all relevant times resided in Rogersville, Missouri. Plaintiff provided her PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

13. Plaintiff Carol Johnson played Zynga games from approximately 2016 to 2018, and the games included *Words with Friends*. Plaintiff's PII was stolen in the Zynga Data Breach. Plaintiff did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. Plaintiff confirmed through the website haveibeenpwned.com that her email was accessed in the Zynga Data Breach.

14. Plaintiff Lisa Thomas is a resident and citizen of Wisconsin and at all relevant times resided in Manitowoc, Wisconsin. Plaintiff provided her PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving

Plaintiff's PII. Plaintiff Thomas also made at least one "in-app" purchase from Zynga, paid for with a debit card linked to her Google Play account.

15. Plaintiff Lisa Thomas played Zynga games from approximately 2014 to 2018 or 2019, and the games included *Words with Friends* and *Draw Something*. Plaintiff's PII was stolen in the Zynga Data Breach. Plaintiff did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. Plaintiff confirmed through the website haveibeenpwned.com that her email was accessed in the Zynga Data Breach.

16. Plaintiff Joseph Martinez IV is a resident and citizen of Colorado and at all relevant times resided in Castle Rock, Colorado. Plaintiff provided his PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

17. Plaintiff Joseph Martinez IV played Zynga games from approximately 2013 until the end of 2019 or early 2020, and the games included *Words with Friends, Words with Friends 2, Solitaire, Draw Something Classic*, and *Zynga Poker,* and he made in-game purchases in *Words with Friends,* and perhaps others. Plaintiff's PII was stolen in the Zynga Data Breach. Plaintiff did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. Plaintiff confirmed through the website haveibeenpwned.com that his email was accessed in the Zynga Data Breach.

18. Plaintiff Daniel Petro is a resident and citizen of the State of Iowa and at all relevant times resided in Des Moines, Iowa. Plaintiff provided his PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

19. Plaintiff Daniel Petro played Zynga games from approximately 2008 to 2018, and the games included *FarmVille, Words with Friends, Mafia Wars,* and *8 Ball Pool,* and he made in-game purchases in *Mafia Wars* and *FarmVille.* Plaintiff did not receive any notice from Zynga, timely or

otherwise, regarding the Zynga Data Breach. Plaintiff confirmed through the website haveibeenpwned.com that his email was accessed in the Zynga Data Breach.

20. Plaintiff Christopher Rosiak is a resident and citizen of the State of Indiana and at all relevant times resided in Dyer, Indiana. Plaintiff provided his PII to Zynga in order to create an account to access and play Zynga games, and did so with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized individuals and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

21. Plaintiff Christopher Rosiak played a Zynga game from approximately December 18, 2011 to no later than 2012, and the game was *Hanging with Friends*. He did not play any other Zynga games, and deleted the application from his phone shortly thereafter. Plaintiff did not receive any notice from Zynga, timely or otherwise, regarding the Zynga Data Breach. Plaintiff learned from IDnotify, an identity theft monitoring service, that his email was accessed in the Zynga Data Breach.

22. Defendant Zynga, Inc. is a Delaware corporation with its headquarters and principal place of business in San Francisco, California.

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative Class members, and Zynga is a citizen of a state different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

24. This Court has personal jurisdiction over Zynga because Zynga is headquartered in this state and regularly transacts business in this state.

25. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district, including decisions made by Zynga related to and led to the Zynga Data Breach alleged herein.

/ / /

IV. FACTS

A. Zynga provides "free" games in exchange for its users' PII.

26. Zynga touts itself as "a leading developer of the world's most popular social games that are played by millions of people around the world each day."[2] Zynga develops, markets, and operates social games as live services played on the Internet, social networking sites, and mobile platforms in the United States and internationally. It offers its online social games under the *Slots, Words with Friends, Zynga Poker*, and *FarmVille* franchises—among many others. Zynga also provides advertising services to advertising agencies and brokers.[3]

27. At the end of 2019, Zynga had an average of an estimated 66 million active users.[4] Zynga's *Words with Friends* was the most popular mobile game in the United States in March 2017, with 13 million unique users for the month. It held that position the prior year, 2016, as well.[5]

28. Zynga's games are accessible on mobile platforms, Facebook, and other social networks, as well as Zynga.com. Zynga offers a mix of paid and "free" games, which are available for download. Zynga's "free" games are supported by in-game advertisements, in-game purchases, and its collection and sale of users' PII.

29. Zynga's exchange of "free" games for its users' PII has been extremely successful. In January 2020, Zynga's CEO claimed that Zynga is "on track to be one of the fastest-growing – if not the fastest-growing – gaming company at scale." In 2019, its stock gained 56%, eclipsing the S&P's 29% increase.[6]

30. To play a Zynga game, the consumer must create a Zynga user account by providing their first name, last name, email address, and gender, and must create a password for the account. At all

---

[2] https://www.zynga.com/# (last visited 3/12/21).
[3] https://www.crunchbase.com/organization/zynga#section-overview (last visited 3/12/21).
[4] "Average monthly active users (MAU) of Zynga games from 4th quarter 2012 to 1st quarter 2020," found at https://www.statista.com/statistics/273569/monthly-active-users-of-zynga-games/ (last visited 3/12/21).
[5] "Words With Friends trumps Pokemon GO as most popular US mobile game in March 2017 with 13 million users" (5/4/17) found at https://www.pocketgamer.biz/news/65662/words-with-friends-13-million-users-march-2017/ (last visited 3/12/21).
[6] "FarmVille Maker Zynga Is Booming Again" (1/3/2020), found at https://www.bloomberg.com/news/articles/2020-01-03/zynga-is-booming-again-after-wilderness-years-at-farmville-maker (last visited 3/12/21).

relevant times and based upon information and belief, Zynga did not collect information regarding a user's age or date of birth and did not require users to verify their age during the registration process. Thus, minors were able to and did create Zynga accounts.

31. Zynga's customers have the option to link their Zynga account to their Facebook account instead of providing an email address, which requires providing Zynga with the user's Facebook username and password. If a prospective mobile user chooses to log in with Facebook, the prospective user must provide their Facebook username and password.

32. Zynga collects and retains its users' names, email addresses, login IDs and passwords, password reset tokens, phone numbers, and Facebook IDs and passwords in its databases. When financial information, such as credit card details, is provided for game purchases or in-app purchases, Zynga retains that information as well.

B. Zynga collected PII from minors.

33. One of Zynga's principal targeted demographics is minor children like Plaintiff I.C.

34. One study estimates that 8% of all mobile gamers are ages 13-17,[7] and based upon information and belief, Zynga is aware that a substantial portion of its user base has been and continues to be minors. If just 8% of Zynga users are minors, that means nearly 14 million children were victims of the September 2019 data breach. In light of the nature of Zynga's available games, the number of affected minors is likely to be much higher in this case.

35. In fact, Zynga acknowledged in Securities and Exchange Commission filings that it is subject to laws and regulations concerning the protection of minors, and that the "increased attention being given to the collection of data from minors" has required it to devote significant operational resources and incur significant expenses.[8]

36. On information and belief, and based on reporting in the media, Zynga is well-aware that a substantial portion of its user base has historically been, and continues to be, comprised of minors, and Zynga has profited handsomely from that user base over the years.

[7] "The Mobile Gaming Industry: Statistics, Revenue, Demographics, More [Infographic]," (2/6/19), found at https://mediakix.com/blog/mobile-gaming-industry-statistics-market-revenue/ (last visited 3/12/21).

[8] Zynga, Inc., Form 10-K, Fiscal Year Ended December 31, 2019, found at https://investor.zynga.com/static-files/d91122ee-c93f-468b-a48e-6d3b3c1441e3 (last visited 3/12/21).

37. Zynga's *PetVille* was the subject of an investigative report which exposed that Facebook targeted Zynga's game-playing minors, and duped those children and their parents out of money, in some cases hundreds or even thousands of dollars, and then refused to refund the amounts.[9]

38. Facebook encouraged game developers such as Zynga to let children spend money without their parents' permission, which Facebook called "friendly fraud," in an effort to maximize revenues.[10] The children oftentimes did not know that they were spending money because while these games are free to download, they are packed with opportunities to spend actual money to advance further. These cash payments are designed to look like items within the game, making it difficult for a child to recognize that they are spending money.[11]

39. Based on their status as minors, Plaintiff I.C. and the Class of minors are not bound by any contractual terms that Zynga forced upon them during the registration process or any time thereafter.

40. Plaintiff I.C. has previously and again hereby disaffirms, repudiates, nullifies, and wishes not to be bound by any and all contracts claimed by Zynga, including the arbitration agreement, terms of service, delegation clause, and all other agreements to which Zynga contends he may be bound.

C. Minors are a high-value target for cyber criminals and are particularly vulnerable to long-term identity theft and PII misuse.

41. According to numerous media reports and studies, stealing the identity of minors is especially attractive to cyber criminals for a host of reasons, including: (1) minors' credit reports are clean, which makes them particularly valuable; (2) minors do not check their credit reports or review monthly bills the way adults do; (3) thieves are more likely to have unfettered access to minors' identity and credit for years or even decades; (4) it is often difficult or impossible to place a freeze on a minor's credit report—because they don't yet *have* credit; and (5) minors are less likely to receive notice, or to have an opportunity to take notice in the event that identity theft occurs or is ongoing, such as, e.g., if

[9] "Facebook knowingly duped game-playing kids and their parents out of money," (1/24/19), found at https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/ (last visited 3/12/21).

[10] *Id*.

[11] "Documents Show Facebook Knowingly Took Money from Unwitting Children," (1/25/19), found at https://www.popularmechanics.com/technology/apps/a26041842/documents-show-facebook-knowingly-took-money-from-unwitting-children/ (last visited 3/12/21).

fraudulent accounts or charges occur under their names, if fake tax returns are filed in their names, if fraudulent health care is obtained under their identity, and if their information is fraudulently used in connection with employment.[12]

42. The Federal Trade Commission agrees that when children are victims of a data breach "it might be years before you or your child realizes there's a problem."[13]

43. For these and other reasons, identity theft is a growing problem in the United States as it relates to our minor population. More than 1 million minors were victims of identity theft or fraud in 2017, totaling $2.6 billion in fraudulent activity.[14]

44. In fact, in 2017, among notified breach victims, 39% of minors became victims of actual fraud (as opposed to 19% of adults).[15]

45. According to a report on child identity theft published by Carnegie Mellon University, a study based on identity protection scans of 40,000 U.S. children, the risk that someone was using their social security number was 51 times higher than the rate for adults in the same population.[16]

46. The Carnegie Mellon report continues: "[t]he potential impact [of identity theft] on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job, or secure a place to live."[17]

47. On information and belief, as a result of their heightened vulnerability and the fact that they are particularly attractive targets for identity thieves, the minors whose data was stolen as a result of the Zynga Data Breach incurred heightened damages.

48. Based on the common use of mobile games among minors, Zynga was well aware of the economic and reputational value of exploiting children for its own monetary gain, and it should have

---

[12] https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html (last visited 3/12/21).

[13] https://www.consumer.ftc.gov/blog/2015/10/protecting-your-childs-information-after-data-breach (last visited 3/12/21).

[14] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (last visited 3/12/21); see also https://www.nbcnews.com/business/consumer/more-1-million-children-were-victims-id-theft-last-year-n885351 (last visited 3/12/21).

[15] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (last visited 3/12/21).

[16] https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 4 (last visited 3/12/21).

[17] *Id.* at 3.

been equally concerned with protecting the PII entrusted to it by that valuable and relatively defenseless group.

D. Zynga's substandard password security; the resulting Data Breach; and Zynga's subsequent failure to reasonably respond and to adequately notify users.

49. On September 29, 2019, The Hacker News reported that a serial hacker from Pakistan called "Gnosticplayers" breached Zynga's user database and improperly accessed and acquired a "massive database" of more than 218 million users. The hacker reported that the breach affected all Android and iOS game players who had installed and signed up for the *Words with Friends* game on or before September 2, 2019. The information stolen included names, email addresses, login IDs, passwords, password reset tokens, phone numbers, Facebook IDs and Zynga account IDs.[18]

50. According to reports, the data breach is known to have included at least the following Zynga games: *Words with Friends*; *Draw Something*; and *OMGPOP*.

51. The Zynga account passwords for those games were secured with SHA-1 cryptography, which is an encryption method that "has been considered outdated and insecure since before Zynga was even founded."[19] SHA-1, or Secure Hash Algorithm 1, "dates back to 1995 and has been known to be vulnerable to theoretical attacks since 2005. The U.S. National Institute of Standards and Technology has banned the use of SHA-1 by U.S. federal agencies since 2010, and digital certificate authorities have not been allowed to issue SHA-1-signed certificates since Jan. 1, 2016…."[20]

52. Other Zynga account passwords for different Zynga games were stored in plain text, and the hacker claimed to have accessed additional data which included clear text passwords for more than 7 million users.[21]

[18] "Exclusive — Hacker Steals Over 218 Million Zynga 'Words with Friends' Gamers Data" (9/29/19), found at https://thehackernews.com/2019/09/zynga-game-hacking.html (last visited 3/12/21).

[19] "Password Breach of Game Developer Zynga Compromises 170 Million Accounts" (12/30/19), found at https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited 3/12/21).

[20] "The SHA1 hash function is now completely unsafe," (2/23/17), found at https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html (last visited 3/12/21).

[21] "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

53. That millions of passwords were maintained in plain text and others in SHA-1 confirms that Zynga had inadequate security measures in place to protect and store its users' PII.

54. Industry watchers have speculated that it is possible that all of Zynga's accounts dating back to the launch of each game accessed by the hacker have been compromised.[22]

55. Zynga knew it was vulnerable to such attacks. As early as 2012, in a Securities and Exchange Commission ("SEC") filing, Zynga reported prior hacking attacks and acknowledged that it "will continue to experience hacking attacks." Zynga recognized that it was "a particularly attractive target for hackers," because of its prominence in the social gaming industry. It reported that it had previously been the subject of "civil claims alleging liability for the breach of data privacy."[23]

56. The Hacker Gnosticplayers, responsible for the Zynga attack, is undoubtedly well-experienced in accessing, acquiring, re-selling, and exploiting stolen PII. Gnosticplayers "is a known quantity in the digital criminal underground, having been observed selling hundreds of millions of breached accounts on the dark web since early 2019."[24] Gnosticplayers had also claimed responsibility for two previous hacking incidents of other websites, one in February 2019 and the second in March 2019, where the hacker put information for millions of accounts for sale on the dark web.[25] "It should be assumed that all of these stolen passwords [from the Zynga Data Breach] will be available in the wild at some point, if they are not already."[26]

57. The number of records stolen as a result of the Data Breach has been reported as ranging between approximately 172–218 million user records. At the time of the Data Breach, according to the website haveibeenpwned.com, the Zynga Data Breach was the tenth largest of all time.[27]

---

[22] *Id.*

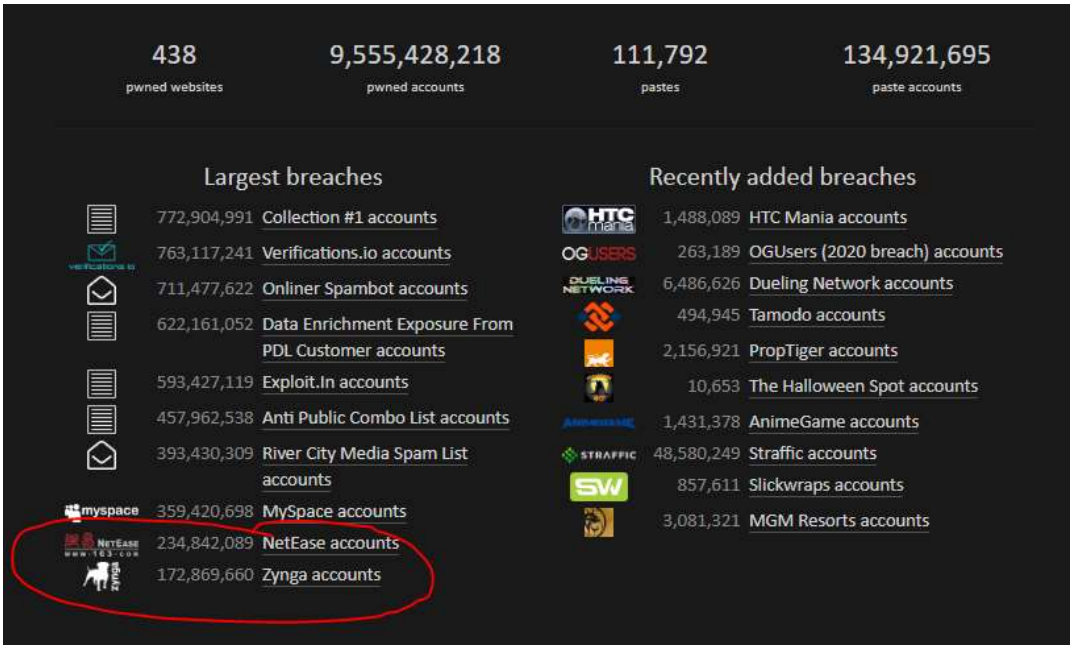
[23] Zynga, Inc., Form 10-K, Fiscal Year Ended December 31, 2012, found at https://www.sec.gov/Archives/edgar/data/1439404/000119312513072858/d489727d10k.htm (last visited 3/12/21).

[24] "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

[25] https://thehackernews.com/2019/09/zynga-game-hacking.html, *supra. See also* "Times when 'Gnosticplayers' hacker made headlines for selling troves of stolen data on dark web," (9/30/19), found at https://cyware.com/news/times-when-gnosticplayers-hacker-made-headlines-for-selling-troves-of-stolen-data-on-dark-web-f8849502 ("Zynga, Inc., and American social game developer is the latest victim of 'Gnosticplayers' hacker") (last visited 3/12/21).

[26] "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

[27] https://haveibeenpwned.com/ (last visited 3/12/21). The website haveibeenpwned.com is a free online resource for an individual to assess if they may have been put at risk due to an online account



58. A search of *Have I Been Pwned* confirms that Plaintiffs' information was exposed as a result of the Zynga Data Breach.[28]

E. Zynga has failed to adequately notify and protect its customers since learning of the Data Breach.

59. In a September 12, 2019 statement posted on its website, called a "Player Security Announcement," Zynga admitted that it had been breached. But Zynga did not accept responsibility for the attack and minimized its scope. Zynga suggested that attacks by hackers are unavoidable: "Cyber attacks are one of the unfortunate realities of doing business today. We recently discovered that certain player account information may have been illegally accessed by outside hackers."[29]

60. Zynga stated, "we do not believe any financial information was accessed. However, we have identified account login information for certain players of *Draw Something* and *Words with Friends* that may have been accessed."[30]

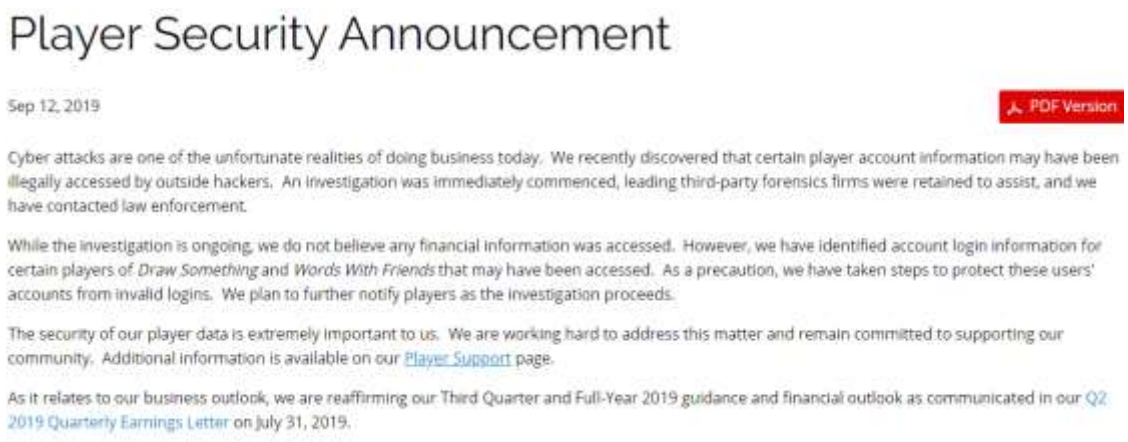
---

having been compromised or "pwned" in a data breach. *See also* https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/, *supra* ("The amount of account records compromised would make this the 10th largest data breach of all time").

[28] *See* https://www.bleepingcomputer.com/news/security/database-from-Zynga-hack-sold-online-check-if-youre-included/ (last visited, August 2019).

[29] https://investor.zynga.com/news-releases/news-release-details/player-security-announcement (last visited 3/12/21).

[30] *Id.*



Player Security Announcement

Sep 12, 2019

PDF Version

Cyber attacks are one of the unfortunate realities of doing business today. We recently discovered that certain player account information may have been illegally accessed by outside hackers. An investigation was immediately commenced, leading third-party forensics firms were retained to assist, and we have contacted law enforcement.

While the investigation is ongoing, we do not believe any financial information was accessed. However, we have identified account login information for certain players of *Draw Something* and *Words With Friends* that may have been accessed. As a precaution, we have taken steps to protect these users' accounts from invalid logins. We plan to further notify players as the investigation proceeds.

The security of our player data is extremely important to us. We are working hard to address this matter and remain committed to supporting our community. Additional information is available on our Player Support page.

As it relates to our business outlook, we are reaffirming our Third Quarter and Full-Year 2019 guidance and financial outlook as communicated in our Q2 2019 Quarterly Earnings Letter on July 31, 2019.

61. Zynga's website announcement – had its customers by chance discovered it – failed to offer its customers resources to manage the fraud and was devoid of any suggestions or instructions about protecting their identities and PII from fraud, such as imposing credit freezes, monitoring credit reports, and checking credit card statements. Instead, Zynga's concern lay with its earnings projections as it concluded its announcement by reaffirming the contents of its "Q2 2019 Quarterly Earnings Letter" dated July 31, 2019.[31]

62. Zynga appears to have discovered the hacking close in time to when it occurred and before the hacking was reported in The *Hacker News*. And while Zynga's website announcement admitted "we have identified account login information for certain players of *Draw Something* and *Words with Friends* that may have been accessed," Zynga never notified those customers by email, or even by a pop-up notification in its gaming applications, so that those customers would be aware of the breach and take timely steps to protect their identities. Instead, it stated that it "plan[s] to further notify players as the investigation proceeds."

63. Zynga had the ability to send an email notification to all users because providing an email address appears to be a universal requirement Zynga imposes on all users when going through the registration process.

64. Rather than sending an email to all users at the time of the breach, Zynga spent its time shoring up its legal defenses.

[31] *Id.*

65. The only alerts some customers may have received came from third-parties such as haveibeenpwned.com—for those few customers who happened to have signed up for automatic notifications from that service. Those alerts were sent on December 18, 2019, three months after Zynga itself was aware of the breach.

66. On that same day, December 18, 2019, whether by design or by coincidence, Zynga modified both its Privacy Policy and Terms of Service.

67. In light of the amount of time that has passed since the data breach, it is "likely that the stolen passwords have been decrypted." An industry expert opined, "The disclosure of the full scale and nature of this breach, some three months after the initial announcement, is concerning. This delay, and the initial lack of information provided by Zynga to its users, has put victims at unnecessary risk."[32]

68. Zynga's conduct leading up to and following the data breach show it is far more concerned with protecting itself than with safeguarding the valuable and confidential information of its users. As noted by one industry expert: "Zynga's response to its breach demonstrates how some organizations tend to view proper security as an afterthought."[33]

69. Zynga released an updated version of its Terms of Service and Privacy Policy on December 18, 2019, the very same day the notification was issued from *Have I Been Pwned*, but still did not send an email to Zynga users alerting them of the breach.

70. Even to this day there may be millions of individuals who do not realize that their PII was stolen as result of the Zynga Data Breach.

71. The PII stolen from Zynga constitutes "personal identifying information," which qualifies as "identity theft" when used to defraud or otherwise misrepresent with the intent of harming the owner of the information. Identity theft can occur by using (with the intent to defraud) information such as: name, birth date, address, phone number, passwords, usernames, or other log-in information that can be used to access a person's electronic content, including content stored on a social networking site.[34]

---

[32] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/, *supra* (quoting Oz Alashe, CEO of CybSafe, a cyber security awareness platform and cloud data analytics platform).

[33] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited 3/12/21).

[34] *See* K.S.A. 21-6107(2).

72. The information stolen from Zynga included names, phone numbers, usernames, email addresses, and passwords—PII that is highly valued amongst cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12), Amazon (≤$10), and Walmart (≤$10) are not far behind. In fact, there is a well-established market for stolen account credentials on the Dark Web, which includes Zynga credentials.

73. One primary concern of the Zynga Data Breach is the use of the username and password combinations in credential stuffing attacks.[35] "Credential stuffing" is when a cyber attacker takes a massive trove of usernames and passwords from a data breach and tries to "stuff" those credentials into the login page of other digital services. Because people frequently use the same username and password across multiple sites, attackers can often use one piece of credential information to unlock multiple accounts.[36]

74. Troy Hunt, a cyber security expert and the founder of *Have I Been Pwned*, has described credential stuffing is a serious threat because: (1) "It's enormously effective due to the password reuse problem"; (2) "It's hard for organisations [sic] to defend against because a successful 'attack' is someone logging on with legitimate credentials"; (3) "It's very easily automatable; you simply need software which will reproduce the logon process against a target website"; and (4) "There are readily available tools and credential lists that enable anyone to try their hand at credential stuffing."[37]

75. In addition to credential stuffing, the breached data includes "enough information for hackers to potentially create targeted phishing attacks made up to look as if they are an official communication from Zynga."[38]

---

[35] *Id.*

36 "Hacker Lexicon: What Is Credential Stuffing?" (2/17/19) found at https://www.wired.com/story/what-is-credential-stuffing/ (last visited 3/12/21).

[37] https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/ (last visited 3/12/21).

[38] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited 3/12/21).

76. The stolen information "is sure to find a home on the dark web, enabling fraudsters to log into user accounts and commit account takeover fraud."[39] Also, "[b]ecause [Zynga] games are often connected to user Facebook accounts, hackers can gain access to far more information under a forged identity."[40] "According to BuiltWith, there are over 190,000 websites that are Facebook Login Button customers and almost 40,000 live websites using Facebook Login Button. Logging in with this stolen information (including the 7 million Draw Something passwords left in clear text with this breach) makes it impossible to determine if the actual account holder is the one logging in."[41]

77. "Compromised pairs of emails and passwords could be injected into commercial websites like Amazon and Ebay in order to fraudulently gain access. The vast majority of email and password combos won't work, but a few will. That's because many people reuse the same credentials on multiple websites."[42]

78. At least one user who created a unique email address to use specifically, and solely for his Zynga account has received multiple fraudulent emails directed to that account that are directly traceable to the Zynga Data Breach.

F. Data breaches, like Zynga's, cause financial, emotional, and physical harm to the victims, including to Plaintiffs and the Class.

79. Annual monetary losses for cybercrimes are estimated to range between $375 billion and $575 billion worldwide. In the United States in 2018, there were 3 million identity theft and fraud complaints filed with the Federal Trade Commission. Of those, 1.4 million were fraud related, and 25% of those reported that money was lost. The median amount consumer paid in those cases was $375.[43]

80. In 2016, more than 25% of identity theft victims had to borrow money from family and friends.[44]

---

[39] *Id*.
[40] *Id*.
[41] *Id*.
[42] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/, *supra* (quoting Oz Alashe).
[43] "Facts + Statistics: Identity theft and cybercrime," found at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited 3/12/21).
[44] "Identity Theft: The Aftermath 2017," p.7, found at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited 3/12/21).

81. But direct, monetary losses are not the only damages that victims of identity theft suffer. According to a Presidential Report on identity theft, victims of identity theft also suffer indirect financial costs, as well as physical and emotional injuries:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[45]

82. The indirect costs of identity theft take victims away from their everyday lives. They spend less time on hobbies and vacations, and are forced to take time off of work and spend time away from their family.

83. The emotional toll that identity theft can take can be grave. Victims suffer from annoyance and frustration, fear of their financial future and financial security, and feel vulnerable, powerless, and helpless. Some seek professional help, and some feel suicidal.[46]

84. "Identity theft can be more than a hassle – replacing credit cards, closing bank accounts, or changing passwords. But for some victims, it can be a life-altering experience that also causes serious emotional problems and can even drive some to consider suicide."[47]

---

[45] "The President's Identity Theft Task Force, Combating Identity Theft, A Strategic Plan" (April 2007), p.11, found at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited 3/12/21).

[46] *Id*.

[47] "Not Just a Financial Toll: Some Victims of Identity Theft Consider Suicide" (11/6/17), found at https://www.nbcnews.com/business/consumer/not-just-financial-toll-some-victims-identity-theft-consider-suicide-n817966 (last visited 3/12/21).

85. There are also physical side-effects that victims of identity theft suffer. Individuals are unable to concentrate or focus, and suffer from fatigue, sleep disturbances, stress, loss of appetite, and an inability to work because of physical symptoms.[48]

86. The physical and emotional responses caused by identity theft can exist for years at a time. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches, use of stolen data can occur years into the future:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[49]

87. Plaintiffs and the Class had their PII stolen in the Zynga Data Breach, causing Plaintiffs and the Class to suffer injuries and damages, including but not limited to the improper disclosure of PII, the loss of value of the PII, ongoing disclosure and dissemination of the PII, the actual and imminent threat of identity theft and other fraud, the loss of privacy, and out-of-pocket expense and time devoted to mitigating the effects of the Data Breach including ascertaining the extent of the Plaintiffs' and the Class's losses and exposure.

88. Plaintiffs and the Class would never have provided their PII to Zynga if Zynga had disclosed that it lacked adequate security measures and data security practices, as was revealed by the media reports.

89. Plaintiffs and the Class have been damaged in that they spent time and resources, and will spend additional time and resources in the future, speaking with representatives; researching and monitoring accounts; researching and monitoring credit history; responding to identity theft incidents; purchasing identity protection; and suffering annoyance, interference, and inconvenience, as a result of the data breach.

90. Zynga's actions and failures to act when required have caused Plaintiffs and the Class to suffer harm and face the significant and imminent risk of future harm, including but not limited to:

---

[48] "Identity Theft: The Aftermath 2017," *supra,* p.12.

[49] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, The Full Extent Is Unknown" GAO Report (June 2007), p.29, found at https://www.gao.gov/assets/270/262899.pdf (last visited 3/12/21).

a. theft of their PII;

b. costs associated with researching the scope and nature of the breach and of responding to the Data Breach and attendant risks and harm in light of Zynga's failure to adequately notify;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. unauthorized access to and misuse of their online accounts;

e. lowered credit scores resulting from credit inquiries and caused by fraudulent activities;

f. costs associated with time spent and the loss of productivity from taking time to address ameliorate, mitigate, and deal with the actual and future consequences of the Zynga Data Breach—including finding fraudulent charges and enrolling in and purchasing credit monitoring and identity theft protection services;

g. the imminent and impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted, directly or indirectly, to Zynga with the mutual understanding that Zynga would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in Zynga's possession and is subject to further breaches so long as Zynga fails to undertake appropriate and adequate measures to protect Plaintiffs and the Class.

91. Consequently, Plaintiffs and the Class are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and Zynga's deceptive and unconscionable conduct.

V. CLASS ACTION ALLEGATIONS

92. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiffs seek certification of the following classes:

93. **Nationwide Class**: All persons residing in the United States whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

94. **Nationwide Adult Subclass:** All adults residing in the United States whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

95. **Nationwide Minor Subclass:** All minors residing in the United States whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019, as well as all individuals in the United States who provided their PII to Zynga while they were minors and had their PII compromised as a result of the Zynga data breach described herein.

96. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff I.C. seeks certification of Kansas state claims in the alternative to the nationwide claims (the "Kansas Subclass"), defined as follows:

97. **Kansas Subclass**: All persons residing in Kansas whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

98. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Gitre seeks certification of Michigan state claims in the alternative to the nationwide claims (the "Michigan Subclass"), defined as follows:

99. **Michigan Subclass**: All persons residing in Michigan whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

100. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Johnson seeks certification of Missouri state claims in the alternative to the nationwide claims (the "Missouri Subclass"), defined as follows:

101. **Missouri Subclass**: All persons residing in Missouri whose PII was obtained or maintained by Missouri and compromised in the Zynga Data Breach that occurred in or around September 2019.

102. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Thomas seeks certification of Wisconsin state claims in the alternative to the nationwide claims (the "Wisconsin Subclass"), defined as follows:

103. **Wisconsin Subclass**: All persons residing in Wisconsin whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

104. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Martinez seeks certification of Colorado state claims in the alternative to the nationwide claims (the "Colorado Subclass"), defined as follows:

105. **Colorado Subclass**: All persons residing in Colorado whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

106. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Petro seeks certification of Iowa state claims in the alternative to the nationwide claims (the "Iowa Subclass"), defined as follows:

107. **Iowa Subclass**: All persons residing in Iowa whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

108. Pursuant to Fed R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff Rosiak seeks certification of Indiana state claims in the alternative to the nationwide claims (the "Indiana Subclass"), defined as follows:

109. **Indiana Subclass**: All persons residing in Indiana whose PII was obtained or maintained by Zynga and compromised in the Zynga Data Breach that occurred in or around September 2019.

110. The Nationwide Class, Nationwide Adult Subclass, the Nationwide Minor Subclass, the Kansas Subclass, the Michigan Subclass, the Missouri Subclass, the Wisconsin Subclass, the Colorado Subclass, the Iowa Subclass, and the Indiana Subclass are collectively referred to herein as the "Class."

111. ***Numerosity: Federal Rule of Civil Procedure 23(a)(1).*** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Over 172 million Zynga accounts in the United States and globally have been exposed, making joinder

impracticable. Those individuals' names, addresses, and email addresses are available from Defendant's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

112. ***Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).*** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendant knew or should have known that its computer and data systems were vulnerable to attack;

b. Whether Defendant acted with intent or reckless indifference with respect to the Class and the safety, value, and security of the Class's PII;

c. Whether the data breach constitutes a breach of the data-security commitments and obligations to protect and safeguard PII made to the Class by Defendant in its privacy policy;

d. Whether Defendant failed to take adequate and reasonable measures to ensure its computer and data systems were protected by, among other things, maintain some passwords in plain text and using outdate encryption methods for others;

e. Whether Defendant failed to take available steps to prevent and stop the breach from happening;

f. Whether Defendant failed to disclose the material facts that it did not have adequate security practices and systems to safeguard its customers' PII;

g. Whether Defendant failed to provide timely and adequate notice of the Data Breach to Plaintiffs and Class members;

h. Whether Defendant owed a duty to Plaintiffs and Class members to protect their PII and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

i. Whether Defendant breached its duties to protect the PII of Plaintiffs and Class members by failing to provide adequate security and by failing to provide timely and accurate notice to Plaintiffs and Class members of the Data Breach;

j. Whether Defendant's actions or inactions resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of Plaintiffs' and Class members' PII;

k. Whether Defendant failed to abide by all applicable legal requirements (including relevant state law requirements) and industry standards concerning the privacy and confidentiality of the Class members' PII;

l. Whether Defendant's conduct violated state consumer protection laws;

m. Whether Defendant's conduct renders it liable for negligence, negligence per se, negligent misrepresentation, breach of contract, breach of implied contract, unjust enrichment, breach of confidence, intrusion upon seclusion, and violations of state statutes;

n. Whether, as a result of Defendant's conduct, Plaintiffs' and Class members' PII was compromised and exposed as a result of the data breach and the extent of that compromise and exposure;

o. Whether, as a result of Defendant's conduct, Plaintiffs and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

p. Whether, as a result of Defendant's conduct, Plaintiffs and Class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief; and

q. Whether, as a result of Defendant's conduct, Plaintiffs and Class members are entitled to damages including, but not necessarily limited to, compensatory damages, punitive damages, costs, and/or attorneys' fees.

113. ***Typicality: Federal Rule of Civil Procedure 23(a)(3).*** Plaintiffs' claims are typical of other Class members' claims because Plaintiffs and Class members were subjected to the same unlawful conduct as alleged herein and injured and damaged in the same manner.

114. ***Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).*** Plaintiffs are adequate class representatives because their interests do not conflict with the interests of Class members

whom they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs' counsel.

115. ***Federal Rule of Civil Procedure 23(b)(1).*** Class action status in this action is warranted under Rule 23(b)(1)(A) because prosecution of separate actions by the members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. Class action status is also warranted under Rule 23(b)(1)(B) because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

116. ***Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).*** Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

117. ***Superiority: Federal Rule of Civil Procedure 23(b)(3).*** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court, especially where there are over 172 million Zynga users affected.

/ / /

VI. CLAIMS

COUNT I - NEGLIGENCE
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes[50] or, Alternatively, on Behalf of Plaintiffs and the State Subclasses[51])

118. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

119. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable and due care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

120. This duty included, among other things:

a. designing, maintaining, and testing its security systems to ensure that Plaintiffs' and Class members' PII in its possession was adequately secured and protected;

b. maintaining security systems consistent with current technology and industry standards, and not storing passwords in plain text or using outdated encryption methods;

c. implementing processes that would detect a breach of its security system in a timely manner;

d. timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks;

e. maintaining data security measures consistent with current technology and industry standards and applicable state and federal law; and

f. timely notifying customers that their PII had been compromised, lost, stolen, accessed, or misused if and when a data breach occurred, notwithstanding (a) through (d) above.

121. Defendant's duty to use reasonable care arose from several sources. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class

[50] "Nationwide Classes" includes the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass as defined herein.

[51] "State Subclasses" includes the Kansas Subclass, the Michigan Subclass, the Missouri Subclass, the Wisconsin Subclass, the Colorado Subclass, the Iowa Subclass, and the Indiana Subclass as defined herein.

members were the foreseeable and probable victims of any inadequate security practices in Defendant's affirmative collection of customers' PII.

122. Zynga solicited, gathered, and stored the PII provided by Plaintiffs and the Class.

123. Defendant knew or should have known it inadequately safeguarded this information.

124. Defendant knew or should have known that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and the Class, and Zynga was therefore charged with a duty to adequately protect this critically sensitive information.

125. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by the Defendant's failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and other Class members would be harmed. Defendant admits as much in its SEC filings.

126. Defendant's duty to Plaintiffs and Class members also arose because of a special relationship that existed between Defendant and Plaintiffs and Class members. That special relationship arose because Plaintiffs and the Class members entrusted Defendant with their PII as part of the creation of user accounts necessary to access Zynga's online and mobile gaming applications. Only Defendant could have ensured that its security systems and data protection measures were sufficient to minimize or prevent the Data Breach.

127. Defendant's duty to Plaintiffs and Class members also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty, including California's Unfair Competition Law.

128. Defendant breached the duties it owed to Plaintiffs and Class members described above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class members; (b) detect the breach while it was ongoing; (c) design and

maintain security systems consistent with current technology and industry standards that could have prevented the loss of data at issue; and (d) timely, adequately and accurately disclose that Plaintiffs' and Class members' PII had been or was reasonably believed to have been, stolen or compromised.

129. Timely notification of the Data Breach was required, appropriate, and necessary so that, among other things, Plaintiffs and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

130. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their PII would not have been compromised.

131. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered economic and non-economic injuries, as follows:

a. theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future

consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. the physical and emotional injuries caused by being victimized by a data breach;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members.

132. Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II - Negligence
(Against Zynga on Behalf of I.C. and the Nationwide Minor Subclass)

133. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

134. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

135. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

136. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's negligence described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

137. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that Zynga collected, and Zynga was aware of the heightened vulnerability and damage that would be suffered by I.C. and the Nationwide Minor Subclass in the event of a data breach.

138. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the minors' PII that Zynga collected.

139. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the Class of a data breach as soon as possible after it is discovered.

140. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass because they were foreseeable and probable victims of any inadequate data security practices.

141. Zynga solicited, gathered, and stored the PII provided by I.C. and the Nationwide Minor Subclass and profited from the same.

142. Zynga knew or should have known it inadequately safeguarded this information.

143. Zynga knew or should have known that a breach of its systems would inflict millions of dollars of damages upon I.C. and the Nationwide Minor Subclass, and Zynga was therefore charged with a heightened duty to adequately protect this critically sensitive information.

144. Zynga had a special relationship with I.C. and the Nationwide Minor Subclass; I.C. and the Nationwide Minor Subclass's willingness to entrust Zynga with their PII was predicated on the understanding that Zynga would take adequate security precautions. Moreover, only Zynga had the ability to protect its systems and the PII it stored on them from attack and Zynga knew of the lack of sophistication and defenselessness of I.C. and the Nationwide Minor Subclass in taking steps to protect themselves in the event of a data breach.

145. Zynga's own conduct also created a foreseeable risk of harm to I.C. and the Nationwide Minor Subclass and their sensitive information. Zynga's misconduct included failing to: (1) secure its systems, despite knowing their unique vulnerabilities, (2) comply with industry standard security

practices for protecting minors' PII, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

146. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of I.C. and the Nationwide Minor Subclass.

147. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by creating a foreseeable risk of harm through the misconduct previously described.

148. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

149. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to timely, adequately, and accurately disclose that I.C. and the Nationwide Minor Subclass's PII had been improperly stolen, acquired, or accessed.

150. The law further imposes a heightened affirmative duty on Zynga to timely disclose the unauthorized access and theft of the PII to I.C. and the Nationwide Minor Subclass so that I.C. and the Nationwide Minor Subclass can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial and sensitive information.

151. Zynga breached its heightened duty to notify I.C. and the Nationwide Minor Subclass by failing to provide I.C. and the Nationwide Minor Subclass with information regarding the breach beyond the inadequate Player Security Update posted on its website. To date, Zynga has not provided sufficient information to I.C. and the Nationwide Minor Subclass regarding the extent of the unauthorized access and continues to breach its disclosure obligations to I.C. and the Nationwide Minor Subclass.

152. As a direct and proximate result of Zynga's negligent conduct, I.C. and the Nationwide Minor Subclass have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III – Negligence Per Se
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

153. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

154. Plaintiffs bring this claim, to the extent necessary, to their claim for Negligence (Count I).

155. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC Act, the unfair act or practice by companies such as Defendant of failing to use reasonable measures to protect PII. This statute, and the various related FTC Act publications and orders, form the basis of Defendant's duty to Plaintiffs in this negligence per se claim.

156. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs' and Class members' PII, failing to use current and generally accepted technology, and not complying with industry standards; by falsely representing to its users and the public the nature and scope of the data breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the size of its customer database, the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach.

157. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

158. Plaintiffs and Class members are not seeking to hold Defendant liable under the FTC Act, itself. Instead, that section forms the basis of Defendants' duty to Plaintiffs and Class members.

159. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

160. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

161. As a result of Defendant's negligence per se, Plaintiffs and Class members have been injured as follows:

a. theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. the physical and emotional injuries caused by being victimized by a data breach;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members.

162. Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT IV – Negligence Per Se – FTC Act
(Against Zynga on Behalf of I.C. and the Nationwide Minor Subclass)

163. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

164. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

165. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

166. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's negligence per se described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

167. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Zynga of failing to use reasonable measures to protect minors' PII. Various FTC publications and orders also form the basis of Zynga's duty.

168. Zynga violated Section 5 of the FTC Act by failing to use reasonable measures to protect minors' PII; by failing to comply with applicable industry standards for protecting minors' PII; by falsely representing to its users and the public the nature and scope of the Data Breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. Zynga's conduct was particularly unreasonable given the vulnerability of the child victims, the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and the foreseeable consequences of misleading its users and the public.

169. Zynga's violation of Section 5 of the FTC Act constitutes negligence per se.

170. I.C. and the Nationwide Minor Subclass are within the category of persons the FTC Act was intended to protect.

171. The harm that occurred as a result of the Data Breach described herein and in the various media reports is the type of harm the FTC Act was intended to guard against.

172. As a direct and proximate result of Zynga's negligence per se, I.C. and the Nationwide Minor Subclass have suffered injury, have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

173. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's negligent misrepresentation than adult victims and are thus entitled to increased damages.

COUNT V – Negligent Misrepresentation
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on behalf of Plaintiffs and the State Subclasses)

174. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

175. Through Zynga's Privacy Policy (the "Privacy Policy") and other actions and representations, Zynga held itself out to Plaintiffs and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII of Plaintiffs and the Class.

176. Based upon information and belief, the Privacy Policy, as it was in effect at the time of the Zynga Data Breach, promised that "[w]e implement reasonable and appropriate security measures to help protect the security of your information both online and offline and to ensure that your data is treated securely."

177. Zynga owed a duty to Plaintiffs and the Class to communicate accurate information about its compliance with the representations made in its Privacy Policy and about any material weaknesses in its data security systems and procedures.

178. Zynga knew or should have known that it was not in compliance with the representations made in its Privacy Policy. This is because Zynga did not maintain security systems consistent with current technology and industry standards, but instead and among other things, maintained passwords in plain text or by using outdated encryption methods.

179. Zynga knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiffs and the Class.

180. Neither Plaintiffs nor the Class could have known or discovered the material weaknesses in Zynga's data security practices.

181. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiffs and the Class.

182. Zynga also failed to exercise reasonable care when it failed to properly communicate information concerning the Data Breach that it knew, or should have known, compromised the PII of Plaintiffs and the Class.

183. Plaintiffs and the Class justifiably relied on Zynga's representations, or lack thereof, when they provided their PII to Zynga.

184. As a direct and proximate result of Zynga's negligent misrepresentation by omission, Plaintiffs and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

COUNT VI – Negligent Misrepresentation
(Against Zynga on behalf of I.C. and the Nationwide Minor Subclass)

185. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

186. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

187. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

188. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's negligent misrepresentation described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

189. Through its Privacy Policy and other actions and representations, Zynga held itself out to I.C. and the Nationwide Minor Subclass as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to I.C. and the Nationwide Minor Subclass.

190. Zynga owed a heightened duty to I.C. and Nationwide Minor Subclass to communicate accurate information about its compliance with the representations made in its Privacy Policy and about any material weaknesses in its data security systems and procedures.

191. Zynga knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

192. Zynga knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to I.C. and the Nationwide Minor Subclass.

193. Neither I.C. nor the Nationwide Minor Subclass could have known or discovered the material weaknesses in Zynga's data security practices.

194. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to I.C. and the Nationwide Minor Subclass.

195. Zynga also breached its heightened duty to I.C. and Nationwide Minor Subclass when it failed to properly communicate information concerning the Data Breach that it knew, or should have known, compromised PII of I.C. and the Nationwide Minor Subclass.

196. I.C. and the Nationwide Minor Subclass justifiably relied on Zynga's representations, or lack thereof, when they provided their PII to Zynga.

197. As a direct and proximate result of Zynga's negligent misrepresentations by omission, I.C. and the Nationwide Minor Subclass have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

198. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's negligent misrepresentation than adult victims and are thus entitled to increased damages.

COUNT VII - Breach of Contract
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

199. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

200. Zynga's Privacy Policy is an agreement between Zynga and persons who provide their PII to Zynga, including Plaintiffs and Class members.

201. Based upon information and belief, the Privacy Policy, as it was in effect at the time of the Zynga Data Breach, promised that "[w]e implement reasonable and appropriate security measures to help protect the security of your information both online and offline and to ensure that your data is treated securely."

202. The Privacy Policy, as it was in effect at the time of the Zynga Data Breach, stated that it applies to persons who use Zynga's services, meaning games, products, services, content, Zynga.com, and/or domain or website operated by Zynga, and it details how Zynga will both protect and use the PII provided by users of Zynga's services.

203. Plaintiffs and Class members on the one hand and Zynga on the other formed a contract when Plaintiffs and Class members provided PII to Zynga subject to the Privacy Policy and used Zynga's services.

204. Plaintiffs and Class members fully performed their obligations under the contract with Zynga.

205. Zynga breached its agreement with Plaintiffs and Class members by failing to protect their PII. Specifically, Defendant (1) failed to use reasonable measures to protect that information by, among other things, not using security systems consistent with current technology and industry standards; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

206. As a direct and proximate result of these breaches of contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, including but not limited to being denied the benefit of the bargain pursuant to which they provided their PII to Zynga.

COUNT VIII - Breach of Implied Contract
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

207. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

208. This claim is an alternative to Plaintiffs' and the Nationwide Class' breach of contract claim.

209. Plaintiffs and Class members alternatively entered into an implied contract with Zynga when they obtained services from Zynga, or otherwise provided PII to Zynga.

210. As part of these transactions, Zynga agreed to safeguard and protect the PII of Plaintiffs and Class members.

211. Plaintiffs and Class members entered into implied contracts with the reasonable expectation that Zynga's data security practices and policies were reasonable and consistent with industry standards. Under the implied contracts, Plaintiffs and Class members believed that Defendant would use part of the monies paid to Zynga or monies it derived from advertising to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

212. Plaintiffs and Class members would not have provided and entrusted their PII to Zynga and/or would have paid less in the absence of the implied contract or implied terms between them and Zynga. The safeguarding of the PII of Plaintiffs and Class members was critical to realize the intent of the parties' bargain.

213. Plaintiffs and Class members fully performed their obligations under the implied contracts with Zynga.

214. Zynga breached its implied contracts with Plaintiffs and Class members by failing to protect their PII. Specifically, Defendant (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the implied agreement.

215. As a direct and proximate result of these breaches of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, including but not limited to being denied the benefit of the bargain pursuant to which they provided their PII to Zynga.

COUNT IX - Unjust Enrichment
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

216. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

217. This claim is an alternative to Plaintiffs' breach of contract and breach of implied contract claims.

218. Plaintiffs and Class members have an equitable and legal interest in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

219. Defendant benefited from the collection of Plaintiffs and the Class' PII, and its ability to retain, use, and profit from that information. Defendant understood the benefit of collecting and possessing this information.

220. Defendant also understood that Plaintiffs' and the Class' PII was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

221. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided, transferred or entrusted their PII to the Defendant, and Zynga would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by Plaintiffs and the Class, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain DT infrastructures, staffing and expertise raising investment capital as described herein, and realizing excessive profits..

222. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and Class members has been diminished.

223. Defendant benefitted by Plaintiffs and Class members' purchases of mobile gaming applications or in-game items, or using Defendant's free gaming applications where paid advertising was displayed, and this benefit was more than those services were worth to Plaintiffs and Class members had been aware that Defendant would fail to protect their PII.

224. Zynga also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

225. It is inequitable for Defendant to retain these benefits.

226. As a result of Defendant's wrongful conduct including, among other conduct, its knowing failure to employ adequate data security measures, its continued maintenance and use Plaintiffs' and Class members' PII without having adequate data security measures, and its other conduct facilitating the theft of that PII, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members.

227. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and thieves.

228. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class members in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

229. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

230. Plaintiffs and Class members have no adequate remedy at law.

231. Defendant is therefore liable to Plaintiffs and Class members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically: the value to Defendant of the PII that was stolen in the Zynga Data Breach; the profits Defendant is receiving from the use of that information; the amount that Zynga overcharged Plaintiffs and Class members for use of its online and mobile gaming application services through in-app purchases; and the amounts that Zynga should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

COUNT X – Unjust Enrichment
(On behalf of I.C. and the Nationwide Minor Subclass)

232. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

233. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

234. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

235. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's unjust enrichment described herein because, without limitation, they are especially:

(1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

236. I.C. and the Nationwide Minor Subclass have an interest, both equitable and legal, in their PII that was collected and maintained by Zynga. This PII was conferred on Zynga directly by I.C. and the Nationwide Minor Subclass themselves.

237. Zynga was benefitted by the conferral upon it of the PII pertaining to I.C. and the Nationwide Minor Subclass and by its ability to retain and use that information. Zynga understood that it was in fact so benefitted.

238. Zynga also understood and appreciated that the PII pertaining to I.C. and the Nationwide Minor Subclass was private and confidential, and its value depended upon Zynga maintaining the privacy and confidentiality of that PII.

239. But for Zynga's willingness and commitment to maintain its privacy and confidentiality, I.C. and the Nationwide Minor Subclass would not have transferred PII to Zynga or entrusted their PII to Zynga, and Zynga would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by I.C. and the Nationwide Minor Subclass, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain DT infrastructures, staffing and expertise raising investment capital as described herein, and realizing excessive profits.

240. As a result of Zynga's wrongful conduct as alleged in this Complaint (including, among other things, its deception of I.C., the Nationwide Minor Subclass, its users in general, and the public relating to the nature and scope of the data breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to I.C. and the Nationwide Minor Subclass without having adequate data security measures; and its other conduct facilitating the theft of

that PII) Zynga has been unjustly enriched at the expense of, and to the detriment of, I.C. and the Nationwide Minor Subclass.

241. Zynga's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of I.C. and the Nationwide Minor Subclass members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

242. Under the common law doctrine of unjust enrichment, it is inequitable for Zynga to be permitted to retain the benefits it received, and is still receiving, without justification, from I.C. and the Nationwide Minor Subclass in an unfair and unconscionable manner. Zynga's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

243. The benefit conferred upon, received, and enjoyed by Zynga was not conferred officiously or gratuitously, and it would be inequitable and unjust for Zynga to retain the benefit.

244. Zynga is therefore liable to I.C. and the Nationwide Minor Subclass for restitution in the amount of the benefit conferred on Zynga as a result of its wrongful conduct, including specifically the value to Zynga of the PII that was stolen in the Zynga data breach and the profits Zynga is receiving from the use and sale of that information.

245. As child victims, I.C. and the Nationwide Minor Subclass conferred a greater benefit on Zynga and suffered greater harm from Zynga's wrongful conduct than adult victims, and as a result, I.C. and the Nationwide Minor Subclass are entitled to increased damages.

COUNT XI – Breach of Confidence
(Against Zynga on Behalf of Plaintiffs and the Nationwide Classes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

246. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

247. At all times, Defendant was aware of the confidential and sensitive nature of Plaintiffs' and Class members' PII.

248. As alleged herein and above, Zynga's relationship with Plaintiffs and Class members was governed by terms of the Privacy Policy and/or the implied expectation that Plaintiffs' and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

249. Plaintiffs' and Class members provided their PII to Zynga with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to the public or any unauthorized parties.

250. Plaintiffs and Class members also provided their respective PII to Zynga with the explicit and implicit understandings that Defendant would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

251. Zynga voluntarily received in confidence Plaintiffs' and Class members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

252. Due to Zynga's failure to prevent, detect, avoid the Data Breach from occurring by following best systems and security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties and the public beyond Plaintiffs' and Class members' confidence, and without their express permission.

253. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Zynga Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

254. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Zynga knew its computer systems for accepting, securing, and storing Plaintiffs' and Class members' PII had serious security vulnerabilities where Zynga failed to observe even basic information security practices or correct known security vulnerabilities.

255. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

/ / /

COUNT XII – Violation of State Data Breach Statutes
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class Residing in States with Applicable Data Breach Statutes or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

256. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

257. This count is brought on behalf of all Class members residing in states with applicable data breach statutes.

258. Zynga is in possession of PII belonging to Plaintiffs and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

259. Despite having email addresses for the individuals whose PII was stolen, Zynga did not provide notification of the breach to the individuals whose PII was stolen.

260. As to applicable state laws, Zynga failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of California, Colorado, Illinois, Iowa, Kansas, Michigan, New Jersey, North Carolina, Wisconsin, and all other applicable State laws.

261. Zynga further failed to provide reasonable and timely notice of the Data Breach to Plaintiffs and the Class as required by the various state data breach notification statutes, including, without limitation, Cal. Civ. Code § 1798.80, et seq.; Colo. Rev. Stat. § 6-1-176; 815 ILCS 530/5, et seq.; Iowa Code Ann. § 715C.2; Kan. Stat. Ann. § 50-7a02; Mich. Comp. Laws Ann. § 445.72; N.J. Stat. § 56:8-163; N.C. Gen. Stat. § 75-61, et seq.; Wis. Stat. §134.98; and other similar state data breach statutes.

262. As a result of Zynga's failure to reasonably safeguard the PII belonging to Plaintiffs and the Class, and Zynga's failure to provide reasonable and timely notice of the Data Breach to Plaintiffs and the Class, Plaintiffs and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

COUNT XIII – Violation of State Data Breach Statutes
(Against Zynga on Behalf of I.C. and the Nationwide Minor Subclass)

263. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

264. This count is brought on behalf of I.C. and the Nationwide Minor Subclass members residing in states with applicable data breach statutes.

265. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

266. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's violation of state data breach statutes described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

267. Zynga is in possession of PII belonging to I.C. and the Nationwide Minor Subclass and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

268. Despite having the email addresses for the individuals whose PII was stolen, Zynga did not provide notification of the breach to the individuals whose PII was stolen.

269. As to applicable state laws, Zynga failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of California, Illinois, New Jersey, North Carolina, and all other applicable State laws.

270. Zynga further failed to provide reasonable and timely notice of the Data Breach to I.C. and the Nationwide Minor Subclass as required by the various state data breach notification statutes, including, without limitation, Cal. Civ. Code § 1798.80 et seq.; 815 Ill. Comp. Stat. 530/5 et seq.; N.J. Stat. § 56:8-163; N.C. Gen. Stat. § 75-61; and other similar state data breach statutes.

271. As a result of Zynga's failure to reasonably safeguard the PII belonging to I.C. and the Nationwide Minor Subclass, and Zynga's failure to provide reasonable and timely notice of the Data

Breach to I.C. and the Nationwide Minor Subclass, I.C. and the Nationwide Minor Subclass have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

272. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's violation of state data breach statutes than adult victims and are thus entitled to increased damages.

COUNT XIV – Intrusion Upon Seclusion
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class who Reside in Intrusion Upon Seclusion States or, Alternatively, on Behalf of Plaintiffs and the State Subclasses)

273. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

274. Plaintiffs bring this claim on behalf of persons who reside in: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

275. Plaintiffs had a reasonable expectation of privacy in the PII that Zynga mishandled.

276. By failing to keep Plaintiffs' PII safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Zynga invaded Plaintiffs' privacy by:

a. intruding into Plaintiffs' private affairs in a manner that would be highly offensive to a reasonable person; and

277. Zynga knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Zynga's actions highly offensive.

278. Zynga invaded Plaintiffs' right to privacy and intruded into Plaintiffs' private affairs by misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

279. As a proximate result of such misuse and disclosures, Plaintiffs' reasonable expectation of privacy in their PII was unduly frustrated and thwarted. Zynga's conduct amounted to a serious invasion of Plaintiffs' protected privacy interests.

280. In failing to protect Plaintiffs' Private Information, and in misusing and/or disclosing their PII, Zynga has acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of users. The Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT XV – Intrusion Upon Seclusion
(Against Zynga on Behalf of I.C. and the Nationwide Minor Subclass who reside in Intrusion Upon Seclusion States)

281. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

282. I.C. and the Nationwide Minor Subclass bring this claim on behalf of minors who reside in: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, West Virginia, and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

283. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

284. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's intrusion upon seclusion described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of

their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

285. I.C. and the Nationwide Minor Subclass had a reasonable expectation of privacy in the PII that Zynga mishandled.

286. By failing to keep I.C.'s and the Nationwide Minor Subclass's Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Zynga invaded I.C.'s and the Nationwide Minor Subclass's privacy by:

287. Intruding into I.C.'s and the Nationwide Minor Subclass's private affairs in a manner that would be highly offensive to a reasonable person; and

288. Zynga knew, or acted with reckless disregard of the fact that, a reasonable person in I.C.'s and the Nationwide Minor Subclass's position would consider Zynga's actions highly offensive.

289. Zynga invaded I.C.'s and the Nationwide Minor Subclass's right to privacy and intruded into their private affairs by misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

290. As a proximate result of such misuse and disclosures, I.C.'s and the Nationwide Minor Subclass's reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Zynga's conduct amounted to a serious invasion of I.C.'s and the Nationwide Minor Subclass's protected privacy interests.

291. In failing to protect I.C.'s and the Nationwide Minor Subclass's Private Information, and in misusing and/or disclosing their Private Information, Zynga has acted with malice and oppression and in conscious disregard of I.C.'s and the Nationwide Minor Subclass's rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of users. I.C. and the Nationwide Minor Subclass, therefore, seek an award of damages, including punitive damages.

292. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's privacy intrusion than adult victims and are thus entitled to increased damages, including punitive damages.

COUNT XVI – Declaratory Judgment
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class)

293. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

294. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

295. An actual controversy has arisen in the wake of the Zynga Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their PII. Plaintiffs and class members remain at imminent risk that further compromises of their PII will occur in the future. This is true even if they are not actively using Defendant's online games or mobile applications.

296. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure customers' PII and to timely notify consumers of a date breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

297. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

298. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Zynga. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

299. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Zynga, Plaintiffs and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

300. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Zynga, thus eliminating additional injuries that would result to Plaintiff, class members, and the millions of consumers whose PII would be further compromised.

COUNT XVII– Declaratory Judgment
(Against Zynga on Behalf of I.C. and the Nationwide Minor Subclass)

301. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

302. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

303. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

304. An actual controversy has arisen in the wake of the Zynga data breach regarding its present and prospective common law and other duties to reasonably safeguard its minor customers' PII and whether Zynga is currently maintaining data security measures adequate to protect I.C. and the Nationwide Minor Subclass from further data breaches that compromise their PII. I.C. and the Nationwide Minor Subclass allege that Zynga's data security measures remain inadequate to protect the PII of minors.

305. I.C. and the Nationwide Minor Subclass continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

306. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Zynga continues to owe a legal duty to secure minor consumers' PII and to timely notify minor consumers of any data breach and that Zynga is required to establish and implement data security measures that are adequate to secure minor consumers' PII.

307. The Court also should issue corresponding prospective injunctive relief requiring Zynga to employ adequate security protocols consistent with law and industry standards to protect minor consumers' PII.

308. If an injunction is not issued, I.C. and the Nationwide Minor Subclass will suffer irreparable injury, and I.C. and the Nationwide Minor Subclass lack an adequate legal remedy. The threat of another Zynga data breach is real, imminent, and substantial. If another breach at Zynga occurs, I.C. and the Nationwide Minor Subclass will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

309. The hardship to I.C. and the Nationwide Minor Subclass if an injunction does not issue exceeds the hardship to Zynga if an injunction is issued. Among other things, if another massive data breach occurs at Zynga, I.C. and the Nationwide Minor Subclass will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Zynga of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Zynga has a pre-existing legal obligation to employ such measures.

310. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Zynga, thus eliminating the additional injuries that would result to I.C. and the Nationwide Minor Subclass and the millions of minor consumers whose confidential information would be further compromised.

COUNT XVIII – Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code, §§ 17200, et seq.
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class)

311. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

312. Defendant violated the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, et seq., by engaging in unlawful, unfair, and deceptive business acts and practices.

313. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

314. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Maintaining passwords in plain text or using outdate encryption methods.

c. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach. This conduct was unfair when weighed against the harm to Plaintiffs and Class members, whose PII has been compromised;

d. Failing to implement and maintain reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;

e. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

f. Failing to implement and maintain reasonable security measures, which led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused;

g. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82, by failing to disclose a data security breach and failing to notify or timely notify Plaintiffs and Class members that their PII had been accessed and stolen;

h. Misrepresenting in in its Privacy Policy and elsewhere that it would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII;

j. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and

k. Failing to notify Plaintiffs and Class members that their PII had been accessed and stolen.

315. Defendant has also engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California False Advertising Law, Cal. Bus. & Prof. Code §§ 17500, et seq., California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

316. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

317. Defendant had exclusive knowledge of material facts not known to Plaintiffs and Class members and Defendant made partial representations but also suppressed some material facts.

318. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and Class members were injured and lost money or property: the money received by Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they

would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

319. Defendant acted intentionally, knowingly, and maliciously to violate California's UCL, and recklessly disregarded Plaintiffs' and Class members' rights and interests. As disclosed in SEC filings, Defendant knew that its security and privacy protections were vulnerable to attack, and Defendant knew that its security measures were inadequate in the face of such attack.

320. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; and other appropriate equitable relief.

COUNT XIX – Violations of the California False Advertising Law
Cal. Bus. & Prof. Code § 17500, et seq.
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class)

321. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

322. Defendant violated the California False Advertising Law ("FAL"), Cal. Bus. & Prof. Code §§ 17500, et seq., by engaging in unlawful, untrue, misleading and deceptive advertising and practices.

323. Section 17500 of the Cal. Bus. & Prof. Code states: "It is unlawful for any . . . corporation . . . with intent directly or indirectly . . . to perform services, professional or otherwise, or anything of any nature whatsoever or to induce the public to enter into any obligation relating thereto, to make or disseminate or cause to be made or disseminated before the public in this state, or to make or disseminate or cause to be made or disseminated from this state before the public in any state, in any newspaper or other publication, or any advertising device, . . . or in any other manner or means whatever, including over the Internet, any statement, concerning that real or personal property or those services, professional or otherwise, or concerning any circumstance or matter of fact connected with the proposed performance or disposition thereof, which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading…."

324. Defendant caused to be made or disseminated through California and the United States, through advertising, marketing and other publications, the following statements or omissions that were untrue or misleading, and which were known, or which by the exercise of reasonable care should have been known to Defendant, to be untrue and misleading to consumers, including Plaintiffs and the other Class members:

a. Failing to disclose that reasonable security measures to protect Plaintiffs' and Class members' PII from unauthorized disclosure, release, data breaches, and theft, were in place, which was a direct and proximate cause of the Data Breach.

b. Failing to disclose foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach. This conduct was unfair when weighed against the harm to Plaintiffs and Class members, whose PII has been compromised;

c. Failing to disclose non-compliance with reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;

d. Failing to disclose non-compliance with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

e. Failing to disclose non-compliance with reasonable security measures, which led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because

consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused;

f. Failing to disclose a data security breach in violation of Cal. Civ. Code § 1798.82, and failing to notify or timely notify Plaintiffs and Class members that their PII had been accessed and stolen;

g. Misrepresenting in in its Privacy Policy and elsewhere that it would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq..

325. Defendant violated § 17500 because the misrepresentations and omissions identified above induced Plaintiffs and the Class to provide their PII to Defendant, and were therefore material and likely to deceive a reasonable consumer.

326. Plaintiffs and Class members have suffered an injury in fact, including the loss of money or property, as a result of Defendant's unlawful, untrue, misleading and deceptive advertising and practices.

327. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

328. Defendant had exclusive knowledge of material facts not known to Plaintiffs and Class members and Defendant made partial representations but also suppressed some material facts.

329. As a direct and proximate result of Defendant's unlawful, untrue, misleading and deceptive advertising and practices, Plaintiffs and Class members were injured and lost money or

property: the money received by Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

330. All of the wrongful conduct alleged herein occurred, and continues to occur, in the conduct of Defendant's business.

331. Defendant's wrongful conduct is part of a pattern or generalized course of conduct that is still perpetuated and repeated, both in the State of California and nationwide.

332. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief;; injunctive relief; and other appropriate equitable relief.

COUNT XX – Violations of the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.
(Against Zynga on Behalf of Plaintiffs and the Nationwide Class)

333. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

334. Defendant violated the California Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, et seq., by engaging in unlawful, untrue, misleading and deceptive advertising and practices.

335. Section 1750 of the California Civil Code provides that certain "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer are unlawful…" Such practices include "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have…" and "[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another…." Cal. Civil Code §1750(a)(5) & (7).

336. Defendant misrepresented the nature of their products and services in violation of the CLRA by engaging in unlawful, unfair, and deceptive acts and practices including:

a. Failing to disclose its failure to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach. This conduct was unfair when weighed against the harm to Plaintiffs and Class members, whose PII has been compromised;

c. Failing to disclose its failure to implement and maintain reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

e. Failing to disclose its failure to implement and maintain reasonable security measures, which led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused;

f. Engaging in unlawful business practices by violating California Civil Code section 1798.82, by failing to disclose a data security breach and failing to notify Plaintiffs and Class members that their PII had been accessed and stolen;

g. Misrepresenting in in its Privacy Policy and elsewhere that it would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII;

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and

j. Failing to notify or timely notify Plaintiffs and Class members that their PII had been accessed and stolen.

337. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiffs and Class members were injured and lost money or property: the money received by Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

338. Defendant acted intentionally, knowingly, and maliciously to violate California's CLRA, and recklessly disregarded Plaintiffs' and Class members' rights and interests. As disclosed in SEC filings, Defendant knew that its security and privacy protections were vulnerable to attack, and Defendant knew that its security measures were inadequate in the face of such attack.

339. Plaintiffs and Class members seek damages stemming from Zynga's unlawful conduct, as well as injunctive relief, declaratory relief, reasonable attorneys' fees and costs, and other appropriate equitable relief.

340. On April 16, 2020, Plaintiffs in the *Martinez* case provided Defendant with notice on behalf of themselves and the Class pursuant to California Civil Code § 1782(a) and various other state statutes, asking Zynga to cease and desist from the fraudulent, unfair, and deceptive business practices, and cure any and all violations forthwith. Zynga failed to take such actions or further respond.

Count XXI – Violations of the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, et seq.
(Against Zynga on Behalf of Plaintiff Carol Johnson and the Missouri Subclass)

341. Plaintiff Johnson realleges and incorporates the foregoing allegations as if fully set forth herein.

342. Defendant violated Mo. Rev. Stat. § 407.010, et seq. ("MMPA") by engaging in unlawful, unfair, unconscionable and deceptive business acts and practices.

343. Defendant's unfair and unconscionable acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Ms. Johnson's and the Missouri Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Ms. Johnson and the Missouri Subclass, whose PII has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and Mo. Rev. Stat. § 407.1500.

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Mo. Rev. Stat. § 407.1500.

344. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Johnson's and the Missouri Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Ms. Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Ms. Johnson's and Missouri Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Ms. Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Ms. Johnson's and the Missouri Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Ms.

Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

345. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

346. As a direct and proximate result of Defendant's unfair, unconscionable, deceptive, and fraudulent acts and practices, Ms. Johnson and the Missouri Subclass members were injured and lost money or property: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

347. Defendant acted intentionally, knowingly, and maliciously to violate Missouri's Merchandising Practices Act, and recklessly disregarded Ms. Johnson's and the Missouri Subclass members' rights. Defendant is of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put it on notice that its security and privacy protections were inadequate.

348. Ms. Johnson and the Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unconscionable, deceptive, and fraudulent business practices for use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

Count XXII – Violations of the Wisconsin Deceptive Trade Practices Act, Wisc. Stat. § 100.18, et seq.
(Against Zynga on Behalf of Plaintiff Lisa Thomas and the Wisconsin Subclass)

349. Plaintiff Thomas realleges and incorporates the foregoing allegations as if fully set forth herein.

350. Zynga is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

351. Ms. Thomas and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

352. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Zynga to members of the public for sale, use, or distribution, Zynga made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

353. Zynga also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

354. Zynga's Deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Thomas' and Wisconsin Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Ms. Thomas' and Wisconsin Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Ms. Thomas' and Wisconsin Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

355. Zynga intended to mislead Ms. Thomas and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

356. Zynga's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Zynga's data security and ability to protect the confidentiality of consumers' PII.

357. Zynga had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the PII in its possession. This duty arose because Ms. Thomas and the Wisconsin Subclass members reposed a trust and confidence in Zynga when they provided their Personal Information to Zynga in exchange for Zynga's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Ms. Thomas and the Wisconsin Subclass—and Zynga, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Zynga. Zynga's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Ms. Thomas and the Wisconsin Subclass that contradicted these representations.

358. Zynga's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

359. Zynga acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Ms. Thomas' and Wisconsin Subclass members' rights. Past data breaches of online businesses, including in the online gaming industry, put Zynga on notice that its security and privacy protections were inadequate.

360. As a direct and proximate result of Zynga's deceptive acts or practices, Ms. Thomas and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

361. Zynga had an ongoing duty to all Zynga customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

362. Ms. Thomas and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

COUNT XXIII – Violations of the Colorado Consumer Protection Act
Colo. Rev. Stat. Ann. § 6-1-101, et seq.
(Against Zynga on Behalf of Plaintiff Joseph Martinez IV and the Colorado Subclass)

363. Plaintiff Martinez realleges and incorporates the foregoing allegations as if fully set forth herein.

364. Defendant violated the Colorado Consumer Protection Act, Colo. Rev. Stat. Ann. § 6-1-101, et seq. by engaging in unfair and deceptive trade practices.

365. Defendant failed to implement and maintain reasonable security measures to protect Mr. Martinez's and the Colorado Subclass members' PII from unauthorized disclosure, release, data

breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents.

366. Defendant engaged in unfair or deceptive trade practices by violating Colo. Rev. Stat. Ann. § 6-1-105, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Martinez's and the Colorado Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Martinez's and the Colorado Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Martinez's and Colorado Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Martinez's and the Colorado Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Martinez's and the Colorado Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr.

Martinez's and the Colorado Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

367. The above practices occurred in the course of Defendant's business, and significantly impacted the public as actual or potential consumers of the Defendant's goods or services.

368. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII, and Plaintiffs and the Colorado Subclass relied on those representations.

369. Defendant intended that the Plaintiffs and Class members would rely on their misrepresentations, omissions, and concealment of information.

370. As a direct and proximate result of Defendant's unfair, unconscionable, deceptive, and fraudulent acts and practices, Mr. Martinez and the Colorado Subclass members suffered an injury in fact to their legally protected interests. Specifically, Mr. Martinez and the Colorado Subclass members were injured and lost money or property: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

371. Mr. Martinez and the Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unconscionable, deceptive, and fraudulent business practices for use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

COUNT XXIV – Violations of the Iowa Consumer Fraud Act
Iowa Code § 714.16, et seq.
(Against Zynga on Behalf of Plaintiff Daniel Petro and the Iowa Subclass)

372. Plaintiff Petro realleges and incorporates the foregoing allegations as if fully set forth herein.

373. Defendant violated the Iowa Consumer Fraud Act, Iowa Code § 714.16, by engaging in the following unlawful business practices:

a. Defendant failed to implement and maintain reasonable security measures to protect Mr. Petro's and the Iowa Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Mr. Petro and the Iowa Subclass, whose PII has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and Iowa Code § 714.16;

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Defendant's concealment, suppression, or omission of material facts referenced above.

374. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Petro's and the Iowa Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Petro's and the Iowa Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Petro's and Iowa Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Petro's and the Iowa Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Petro's and the Iowa Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Petro's and the Iowa Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

375. The above practices occurred in the course of Defendant's business, and significantly impacts the public as actual or potential consumers of the Defendant's goods or services.

376. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII, and Plaintiffs and the Iowa Subclass relied on those representations.

377. Defendant intended that the Plaintiffs and Class members would rely on their misrepresentations, omissions, and concealment of information.

378. As a direct and proximate result of Defendant's unfair, unconscionable, deceptive, and fraudulent acts and practices, Mr. Petro and the Iowa Subclass members suffered an injury in fact to

their legally protected interests. Specifically, Mr. Petro and the Iowa Subclass members were injured and lost money or property: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

379. Mr. Petro and the Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unconscionable, deceptive, and fraudulent business practices for use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

380. On April 14, 2020, pursuant to Iowa Code § 714H.7 and prior to filing suit, Plaintiffs in the *Martinez* case provided the Iowa Attorney General with a draft complaint and requested approval of that office prior to filing. On that same day, the Iowa Attorney General approved of filing the *Martinez* complaint pursuant to Iowa Code § 714H.7.

Count XXV - Indiana Deceptive Consumer Sales Act
Ind. Code § 24-5-0.5-1, et seq.
(Against Zynga on Behalf of Plaintiff Christopher Rosiak and the Iowa Subclass)

381. Plaintiff Rosiak realleges and incorporates the foregoing allegations as if fully set forth herein.

382. Zynga is a "supplier" that engaged in a "consumer transaction" as defined by Ind. Code § 24-5-0.5-2(a)(3), (1), respectively.

383. Mr. Rosiak and the Indiana Subclass members are "persons" as defined by Ind. Code § 24-5-0.5-2(a)(2).

384. Defendant violated the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3, by engaging in unfair and deceptive practices, including:

a. Defendant failed to implement and maintain reasonable security measures to protect Mr. Rosiak's and the Indiana Subclass members' PII from unauthorized

disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Mr. Rosiak and the Indiana Subclass, whose PII has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and Ind. Code § 24-5-0.5-1, et seq;

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused;

d. Defendant's concealment, suppression, or omission of material facts referenced above; and

e. Engaging in deceptive acts as defined by Ind. Code § 24-5-0.5-3.

385. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Rosiak's and the Indiana Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Rosiak's and the Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Rosiak's and Indiana Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Rosiak's and the Indiana Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Rosiak's and the Indiana Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Rosiak's and the Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

386. The above practices occurred in the course of Defendant's business, and significantly impacts the public as actual or potential consumers of the Defendant's goods or services.

387. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII, and Plaintiffs and the Indiana Subclass relied on those representations.

388. Defendant intended that the Plaintiffs and Class members would rely on their misrepresentations, omissions, and concealment of information.

389. As a direct and proximate result of Defendant's unfair, unconscionable, deceptive, and fraudulent acts and practices, Mr. Rosiak and the Indiana Subclass members suffered an injury in fact to their legally protected interests. Specifically, Mr. Rosiak and the Indiana Subclass members were injured and lost money or property: the money received by the Zynga for its services; the loss of the

benefit of their bargain with and overcharges by Zynga as they would not have provided their PII to Zynga and/or paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

390. Mr. Rosiak and the Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unconscionable, deceptive, and fraudulent business practices for use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

391. On April 16, 2020, Plaintiffs in the *Martinez* case provided Defendant with notice on behalf of themselves and the Class pursuant to Ind. Code § 24-5-0.5-5 and various other state statutes, asking Zynga to cease and desist from the fraudulent, unfair, and deceptive business practices, and cure any and all violations forthwith. Zynga failed to take such actions or further respond.

COUNT XXVI – Violations of the Kansas Consumer Protection Act, Kan. Stat. Ann. §§ 50-626(a) and (b)(1)(A)(D) (Against Zynga on Behalf of Plaintiff I.C. and the Kansas Class)

392. Plaintiff I.C. realleges and incorporates by reference the allegations contained in the above paragraphs, as if fully set forth herein.

393. Defendant violated Kan. Stat. Ann. §§ 50-626(a) and (b)(1)(A)(D) and Kan. Stat. Ann. § 50-627(a) by engaging in unlawful, unfair, unconscionable and deceptive business acts and practices.

394. Plaintiffs and Class members are consumers who purchased products from, and/or transacted with, Defendant primarily for personal, family or household purposes.

395. Defendant is a "person" as defined in the relevant state consumer statutes.

396. Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and Class members. Defendant is engaged in, and its acts and omissions affect, trade and commerce.

397. Defendant's acts, practices and omissions were done in the course of Defendant's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

398. Defendant's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the e-commerce industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including but not limited to duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Kansas Subclass members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII.

399. By engaging in such conduct and omissions of material facts, Defendant has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "property or services are of particular standard, quality, grade, style or model, if they are of another

which differs materially from the representation", and/or engaging in an "unconscionable act or practice in connection with a consumer transaction"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

400. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiffs' and Class Members' PII.

401. Defendant intentionally, knowingly, and maliciously misled Plaintiffs and Class Members and induced them to rely on its misrepresentations and omissions.

402. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class Members' PII as part of the services Defendant provided and for which Plaintiffs and Class members paid without advising Plaintiffs and Class members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class members' PII. Accordingly, Plaintiffs and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

403. Past breaches within the e-commerce industry put Defendant on notice that its security and privacy protections were inadequate.

404. Defendant's practices were also contrary to public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures.

405. The harm these practices caused to Plaintiffs and the Class members outweighed their utility, if any, and only caused harm to Plaintiffs and Class members.

406. The injuries, damages, and losses, including to their money, property, and/or the right to privacy suffered by Plaintiffs and Class members as a direct result of Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth in this Complaint include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Defendant data breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Defendant data breach;

f. the imminent, ongoing, and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused via the sale of consumers' information on the dark web;

g. damages to and diminution in value of their personal and financial information entrusted to Defendant for the purpose of purchasing products from Defendant and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others;

h. money paid for products purchased from Defendant during the period of the Defendant breach in that Plaintiffs and Class members would not have purchased from Defendant had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information

and had Defendant provided timely and accurate notice of the Defendant data breach;

i. overpayments made to Defendant for transactions during the Defendant data breach in that a portion of the price for such products paid by Plaintiffs and the Class members to Defendant was for the costs of Defendant providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Defendant failed to do and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Defendant; and

j. the continued risk to their personal information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

407. Defendant's conduct described in this Complaint, including without limitation, Defendant's failure to maintain adequate computer systems and data security practices to safeguard customers' PII, Defendant's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect users' PII, Defendant's failure to provide timely and accurate notice to Consumer Plaintiffs and Class members of the material fact of the Defendant data breach, and Defendant's continued acceptance of Consumer Plaintiffs' and Class members' PII, including credit and banking information for transactions on Defendant after Defendant knew or should have known of the data breach, constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of The Kansas Consumer Protection Act, Kan. Stat. Ann. §§ 50-623 to 50-643.

408. Defendant has long had notice of Plaintiffs' allegations, claims and demands including from the filing of numerous actions by various consumer plaintiffs against Defendant arising from the data breach.

409. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; statutory damages; declaratory and injunctive relief, including an

injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is allowable by law.

COUNT XXVII – Violations of the Michigan Consumer Protection Act M.C.P.A. § 445.903(1)(c)(e),(s) and (cc), et seq. (Against Zynga on Behalf of Plaintiff Amy Gitre and the Michigan Subclass)

410. Plaintiff Amy Gitre realleges and incorporates by reference the allegations contained in the above paragraphs, as if fully set forth herein.

411. Defendant violated the Michigan Consumer Protection Act ("Act"), M.C.P.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*, by engaging in unlawful, unfair, unconscionable and deceptive business acts and practices under the Act.

412. Plaintiffs and Class members are consumers who purchased products from, and/or transacted with, Defendant primarily for personal, family or household purposes.

413. Defendant is a "person" as defined in the relevant state consumer statutes.

414. Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and Class members. Defendant is engaged in, and its acts and omissions affect, trade and commerce.

415. Defendant's acts, practices and omissions were done in the course of Defendant's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

416. Defendant's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the e-commerce industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class members' PII, including but not limited to duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' PII, including by implementing and maintaining reasonable security measures

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Michigan Subclass members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII.

417. By engaging in such conduct and omissions of material facts, Defendant has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another", failing to "reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer", failing to "reveal facts that are material to the transaction in light of representations of fact made in a positive manner", and/or engaging in an unconscionable act or practice in connection with a consumer transaction; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices. *See* M.C.P.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*

418. Defendant's representations and omissions were material because they were likely to deceive, and in fact did deceive, reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiffs' and Class Members' PII.

419. Defendant intentionally, knowingly, and maliciously misled Plaintiffs and Class Members and induced them to rely on its misrepresentations and omissions.

420. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class Members' PII as part of the services Defendant provided and for which Plaintiffs and Class members paid without advising Plaintiffs and Class members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class members' PII. Accordingly, Plaintiffs and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

421. Past breaches within the e-commerce industry put Defendant on notice that its security and privacy protections were inadequate.

422. Defendant's practices were also contrary to public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures.

423. The harm these practices caused to Plaintiffs and the Class members outweighed their utility, if any, and only caused harm to Plaintiffs and Class members.

424. The injuries, damages, and losses, including to their money, property, and/or the right to privacy suffered by Plaintiffs and Class members as a direct result of Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth in this Complaint include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Defendant data breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Defendant data breach;

f. the imminent, ongoing, and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused via the sale of consumers' information on the dark web;

g. damages to and diminution in value of their personal and financial information entrusted to Defendant for the purpose of purchasing products from Defendant and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others;

h. money paid for products purchased from Defendant during the period of the Defendant breach in that Plaintiffs and Class members would not have purchased from Defendant had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Defendant provided timely and accurate notice of the Defendant data breach;

i. overpayments made to Defendant for transactions during the Defendant data breach in that a portion of the price for such products paid by Plaintiffs and the Class members to Defendant was for the costs of Defendant providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Defendant failed to do and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Defendant; and

j. the continued risk to their personal information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

425. Defendant's conduct described in this Complaint, including without limitation, Defendant's failure to maintain adequate computer systems and data security practices to safeguard customers' PII, Defendant's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect users' PII, Defendant's failure to provide timely and accurate notice to Consumer Plaintiffs and Class members of the material fact of the Defendant data breach, and Defendant's continued acceptance of Consumer Plaintiffs' and Class members' PII, including credit and banking information for transactions on Defendant after Defendant knew or should have known of the data breach, constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the Michigan Consumer Protection Act, M.C.P.A. § 445.903(1)(c)(e),(s) and (cc), *et seq*.

426. Defendant has long had notice of Plaintiffs' allegations, claims and demands including from the filing of numerous actions by various consumer plaintiffs against Defendant arising from the data breach.

427. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; statutory damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is allowable by law.

WHEREFORE, Plaintiffs respectfully request that this Court:

a. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs is a proper class representative; and appoint Plaintiffs' counsel as Class Counsel;

b. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. Award Plaintiffs and Class members all damages they are entitled to, including but not limited to compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

d. Award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

e. Grant declaratory relief sought herein;

f. Award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

g. Award pre- and post-judgment interest at the maximum legal rate; and

h. Grant all such other relief as is just and proper.

JURY DEMAND

Plaintiffs demands a trial by jury on all claims so triable.

DATED: March 12, 2021

Respectfully submitted,

By: */s/ Adam J. Zapala*

Adam J. Zapala (SBN 245748)
Reid Gaa (SBN 330141)
COTCHETT, PITRE & McCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 64010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
azapala@cmplegal.com
rgaa@cmplegal.com

Scott C. Nehrbass *(pro hac vice)*
Daniel J. Buller *(pro hac vice)*
FOULSTON SIEFKIN LLP
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway

Overland Park, KS 66210-2000
Tel: (913) 253-2144
Fax: (866) 347-1472
snehrbass@foulston.com
dbuller@foulston.com

E. Powell Miller *(pro hac vice)*
Sharon S. Almonrode *(pro hac vice)*
William Kalas *(pro hac vice pending)*
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com

Attorneys for Plaintiffs I.C., Amy Gitre, and the Proposed Class

Hassan A. Zavareei (State Bar No. 181547)
Mark Clifford (*pro hac vice)*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
hzavareei@tzlegal.com
mclifford@tzlelegal.com

Attorneys for Plaintiffs Carol Johnson and Lisa Thomas, and the Proposed Class

Jennie Lee Anderson (SBN 203586)
ANDRUS ANDERSON LLP
155 Montgomery Street, Suite 900
San Francisco, CA 94104
Telephone: (415) 986-1400
Facsimile: (415) 986-1474
jennie@andrusanderson.com

Elizabeth A. Fegan (pro hac vice)
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com

Lynn A. Ellenberger (*pro hac vice)*

FEGAN SCOTT LLC
500 Grant St., Suite 2900
Pittsburgh, PA 15219
Telephone: (412) 346-4104
Facsimile: (312) 264-0100
lynn@feganscott.com

J. Barton Goplerud (motion for pro hac vice forthcoming)
SHINDLER, ANDERSON, GOPLERUD & WEESE, P.C.,
5015 Grand Ridge Drive, Suite 100
West Des Moines, IA 50265
Telephone: (515) 223-4567
Facsimile: (515) 223-8887
goplerud@sagwlaw.com

Attorneys for Plaintiffs Joseph Martinez IV, Daniel Petro, Christopher Rosiak, and the Proposed Class